JOURNAL OF NUMBER THEORY **58**, 46–54 (1996)
ARTICLE NO. 0059

On a Question of Davenport

PETER MÜLLER*

Mathematisches Institut, Universität Erlangen-Nürnberg, Bismarckstrasse $1\frac{1}{2}$, D-91054 Erlangen, Germany

AND

HELMUT VÖLKLEIN†

Department of Mathematics, University of Florida, Gainesville, Florida 32611

Let k be a number field and denote by $\mathfrak{o}_k$ its ring of integers. Let $\mathfrak{p}$ be a non-zero prime ideal of $\mathfrak{o}_k$. Denote by $\bar{f}$ the polynomial derived from f by reducing the coefficients modulo $\mathfrak{p}$. Set $V_{\mathfrak{p}}(f) = \{\bar{f}(u) \mid u \in \mathfrak{o}_k/\mathfrak{p}\}$. Davenport raised the following question (with k being the rationals). Suppose f and g are polynomials in $\mathfrak{o}_k[X]$ such that $V_{\mathfrak{p}}(f) = V_{\mathfrak{p}}(g)$ for all but finitely many non-zero prime ideals of $\mathfrak{o}_k$. Does this imply $f(X) = g(aX+b)$ for some $a, b \in k$? Extending work of M. Fried, we give an affirmative answer under rather general conditions, and also new types of counter-examples. © 1996 Academic Press, Inc.

1. INTRODUCTION

Let k be a number field and denote by $\mathfrak{o}_k$ its ring of integers. We are interested in the value sets of $f \in \mathfrak{o}_k[X]$ on the residue fields of $\mathfrak{o}_k$. More precisely: Let $\mathfrak{p}$ be a non-zero prime ideal of $\mathfrak{o}_k$. Denote by $\bar{f}$ the polynomial derived from f by reducing the coefficients modulo $\mathfrak{p}$. Set $V_{\mathfrak{p}}(f) = \{\bar{f}(u) \mid u \in \mathfrak{o}_k/\mathfrak{p}\}$.

QUESTION. *Let $f, g \in \mathfrak{o}_k[X]$ such that $V_{\mathfrak{p}}(f) = V_{\mathfrak{p}}(g)$ for all but finitely many non-zero prime ideals of $\mathfrak{o}_k$. Does this imply $f(X) = g(aX+b)$ for some $a, b \in k$?*

* E-mail: mueller@mi.uni-erlangen.de.
† E-mail: helmut@math.ufl.edu.

0022-314X/96 $18.00

The original question of Davenport is in the case $k = \mathbb{Q}$.

The answer is affirmative if $k = \mathbb{Q}$ and f is indecomposable or has odd prime power degree, see [6]. However, for $k \neq \mathbb{Q}$ there are counterexamples even for indecomposable polynomials f, as M. Fried proved, see [8] and Section 6. If $k = \mathbb{Q}$, then the answer is also not generally affirmative—a simple counterexample is given by $f(X) = X^8$, $g(X) = 16X^8$.

In this paper we give an affirmative answer for a large class of decomposable polynomials, namely those satisfying condition $(*)$ below. Using further examples in Section 6 we show that our results are sharp. Our study of indecomposable polynomials amounts to studying certain imprimitive permutation groups. Section 5 contains the group theoretic version of Davenport's question.

2. Kronecker Equivalence of Polynomials

Let f and g be polynomials in $k[X]$, where k is a field of characteristic 0. Let E be a field containing k. Choose a transcendental t and fix a Galois extension Ω of $E(t)$ that contains elements x and y with $f(x) - t = 0$ and $g(y) - t = 0$. Denote by G the Galois group of $\Omega \mid E(t)$. Then f and g are said to be *Kronecker equivalent over* E if the following holds for every element of G. It fixes a root of $f(X) - t = 0$ if and only if it fixes a root of $g(Y) - t = 0$.

In group-theoretic terms: Let U and V be the stabilizers of x and y in G, respectively. Then f and g are Kronecker equivalent if and only if $\bigcup_{g \in G} U^g = \bigcup_{g \in G} V^g$.

Clearly, the definition of Kronecker equivalence does not depend on the choice of Ω. If $E_1 \subseteq E_2$, then Kronecker equivalence over E_1 implies Kronecker equivalence over E_2.

The key for attacking the Davenport problem is

2.1. Theorem [4, Lemma 19.27]. *Let k be a number field and $f, g \in \mathfrak{o}_k[X]$. Then $V_{\mathfrak{p}}(f) = V_{\mathfrak{p}}(g)$ for all but finitely many non-zero prime ideals of $\mathfrak{o}_k$ if and only if f and g are Kronecker equivalent over k.*

3. Monodromy Groups

In order to formulate our main result, we need some definitions. The monodromy group of $f(X) \in E[X]$ is the Galois group of the polynomials $f(X) - t$ over $\bar{E}(t)$. If $a \neq 0$, b, and c are complex numbers and $n \in \mathbb{N}$, then we call the polynomial $(aX + b)^n + c$ *cyclic*. The reason for this

is that its monodromy group is cyclic. Similarly, we call the polynomial $a \cdot T(bX+c)+d$ *dihedral*, where T is defined by $T(Z+1/Z) = Z^n + 1/Z^n$. (T is one of the definitions of a Tchebychev Polynomial.) Two polynomials f and g in $E[X]$ are said to be *linearly related* over E if there are $a, b \in E$, $a \neq 0$, with $f(X) = g(aX+b)$.

A polynomial $f \in k[X]$ is said to be indecomposable over k, if it is not the composition of two non-linear polynomials in $k[X]$. We use the fact that if $\mathrm{char}(k) = 0$ then f is indecomposable over k if and only if it is indecomposable over any extension of k, see [9, Theorem 3.5]. Thus in the following we drop the phrase "over k".

We use the following consequence of a Theorem of Ritt, see [12], or [1] for a modern account.

3.1. THEOREM (Ritt). *Let $f_1 \circ f_2 \circ \cdots \circ f_r = g_1 \circ g_2 \circ \cdots \circ g_s$ be two decompositions into non-linear indecomposable polynomials from $\mathbb{C}[X]$. Assume that no f_i is a cyclic or dihedral polynomial. Then $r = s$ and $f_i = L_{i-1}^{-1} \circ g_i \circ L_i$ with linear polynomials L_i. In particular, the monodromy groups of f_i and g_i are canonically permutation equivalent.*

Further, we need the following well-known fact, see [5].

3.2. LEMMA. *If $f \in \mathbb{C}[X]$ is indecomposable, then its monodromy group is either non-solvable or cyclic, dihedral or S_4.*

Actually, the monodromy groups of indecomposable polynomials have been completely classified as a consequence of the classification of finite simple groups, see [11].

4. RESULTS

We consider the following condition on a polynomial $f \in \mathbb{C}[X]$:

> f can be written as the composition of non-linear indecomposable polynomials none of which is cyclic, dihedral, or has degree 4. (*)

We call a polynomial $f \in \mathbb{C}[X]$ a Davenport polynomial if there is another polynomial $g \in \mathbb{C}[X]$ which is Kronecker equivalent to f (over $\mathbb{C}$), but not linearly related (over $\mathbb{C}$) to f. A clever elementary argument shows that an indecomposable Davenport polynomial cannot have rational coefficients [6, Section 3]. Using the classification of finite simple groups, W. Feit showed there are exactly six families of indecomposable Davenport polynomials, of degree 7, 11, 13, 15, 21, and 31, respectively. See [2] together with [3, Theorem 4.1].

4.1. THEOREM. *Let $f, g \in \mathbb{C}[X]$ be polynomials that are Kronecker equivalent over $\mathbb{C}$. If f satisfies $(*)$, then the following holds*

(1) *If $f, g \in \mathbb{Q}[X]$, then there exists $a, b \in \mathbb{Q}$ with $f(X) = g(aX+b)$.*

(2) *If none of the f_i is a Davenport polynomial, then there exist $a, b \in \mathbb{C}$ with $f(X) = g(aX+b)$.*

From Theorem 2.1 we immediately get

4.2. COROLLARY. *Let k be a number field and $f, g \in \mathfrak{o}_k[X]$. Suppose $V_{\mathfrak{p}}(f) = V_{\mathfrak{p}}(g)$ for all but finitely many-zero prime ideals of $\mathfrak{o}_k$. If f satisfies $(*)$, then the following holds*

(1) *If $f, g \in \mathbb{Q}[X]$, then there exist $a, b \in \mathbb{Q}$ with $f(X) = g(aX+b)$.*

(2) *If none of the f_i is a Davenport polynomial, then there exist $a, b \in \mathbb{C}$ with $f(X) = g(aX+b)$.*

Proof of Theorem 4.1. Set $E = \mathbb{Q}$ or $E = \mathbb{C}$, according to (1) or (2). We use the group-theoretic Lemma 5.1 from the next section. Pick x and y in an algebraic closure of $\mathbb{C}(t)$ such that $f(x) = g(y) = t$. Denote by Ω the Galois closure of $\mathbb{C}(x, y) | \mathbb{C}(t)$. Set $G = \mathrm{Gal}(\Omega | \mathbb{C}(t))$ and let U and V be the fix groups of $\mathbb{C}(x)$ and $\mathbb{C}(y)$ respectively. Then 5.1(iii) holds, as f and g are Kronecker equivalent.

Let Z be the inertial group (= stabilizer) in G of a place of Ω lying over the place of $\mathbb{C}(t)$ at infinity. Then 5.1(i) and (ii) hold (because $\mathbb{C}(x) | \mathbb{C}(t)$ and $\mathbb{C}(y) | \mathbb{C}(t)$ are totally ramified at infinity).

Let L and M be as in 5.1(iv). Then there are polynomials $f^{(1)}$, $f^{(2)}$, $f^{(3)} \in E[X]$, such that $f(X) = f^{(1)}(f^{(2)}(f^{(3)}(X)))$ and $f^{(2)}$ is indecomposable with monodromy group $\bar{M}$, see [9, Theorem 3.4]. By the hypothesis $(*)$ on f, Theorem 3.1, and Lemma 3.2 we get that $\bar{M}$ is not solvable.

Suppose that $\bar{M}$ doesn't meet the requirement 5.1(iv). Then $f^{(2)}$ is a Davenport polynomial, because it follows from the classification of the finite doubly transitive groups, which contain a regular cyclic subgroup [3, Theorem 4.1], that if $\bar{B}_1$ and $\bar{B}_2$ are two complements to $\overline{Z \cap M}$ in $\bar{M}$, then $\bigcup_{g \in \bar{M}} B_1^g = \bigcup_{g \in \bar{M}} B_2^g$. This contradicts the assumption in (2). In case (1) with $E = \mathbb{Q}$, we use Fried's result that $f^{(2)} \in \mathbb{Q}[X]$ is impossible, see [6, Section 3].

Thus all conditions are fulfilled, so we get $U = V^\alpha$ for some $\alpha \in G$. Thus $y^\alpha \in \mathbb{C}(x)$, i.e. $f(x) = t = g(y^\alpha) = g(r(x))$ for some rational function $r \in \mathbb{C}(X)$. Clearly r must be a polynomial, and $\deg(f) = \deg(g) \cdot \deg(r)$. But $\deg(f) = [G : U] = [G : V] = \deg(g)$, hence r is linear.

Thus we are done in case (2), and it remains to show that f and g are linearly related even over $\mathbb{Q}$ in (1). Set $n = \deg(f) = \deg(g)$. The polynomials f and g are linearly related (over $\mathbb{Q}$) to polynomials $\tilde{f}$ and $\tilde{g}$, respectively,

such that the coefficients of X^{n-1} of the latter two polynomials vanish. Then $\tilde{f}(X) = \tilde{g}(cX + d)$ with $c, d \in \mathbb{C}$. It follows that $d = 0$. Compare the highest coefficient of the polynomials to get $c^n \in \mathbb{Q}$. Let e be the smallest positive integer with $c^e \in \mathbb{Q}$. Then $\tilde{f}, \tilde{g} \in \mathbb{Q}[X]$ implies $\tilde{f}(X) = h(X^e)$ for some $h \in \mathbb{Q}[X]$. But the assumption about f implies $e = 1$, hence $c \in \mathbb{Q}$. Therefore f and g are linearly related over $\mathbb{Q}$. ▮

5. A Group-Theoretic Lemma

If G is a group and H is a subgroup, then $\mathrm{core}_G(H)$ denotes the intersection on the conjugates of H in G.

5.1. Lemma. *Let G be a finite group with subgroups U, V, and Z such that*

(i) *Z is cyclic*

(ii) $G = UZ = VZ$

(iii) $\bigcup_{g \in G} U^g = \bigcup_{g \in G} V^g$

(iv) *For any groups L and M with $U \leqslant L < M \leqslant G$ and L maximal in M the following holds: Let $g \mapsto \bar{g}$ denote the canonical homomorphism from M to $\bar{M} := M/\mathrm{core}_M(L)$. Then $\bar{M}$ is not solvable and there is at most one $\bar{M}$-conjugacy class of subgroups $\bar{B}$ of $\bar{M}$ with $\bar{M} = \bar{B}(\overline{Z \cap M})$.*

Then $U = V^g$ for some $g \in G$.

Remark. The Theorem is wrong if we drop one of the two conditions on $\bar{M}$ in (iv), see the discussion of counter-examples in 6.

Proof. We study a counter-example with $|G|$ minimal.

Step 1. If $N \lhd G$ with $1 \neq N$, then $UN = V^g N$ for some $g \in G$.

Proof. This follows from the minimality of $|G|$ once we know that the hypotheses (i) to (iv) remain satisfied if we consider the configuration modulo N. This is clear for (i), (ii), and (iii). For (iv) use the canonical isomorphism between the lattice of subgroups of G/N and the lattice of subgroups of G containing N. ▮

In the sequel we frequently use the following consequence of condition (ii): If M is a subgroup of G containing U, then $\{M^g \mid g \in G\} = \{M^z \mid z \in Z\}$. In particular, $Z \cap M \leqslant \mathrm{core}_G(M)$. The same holds for V instead of U.

Step 2. $\mathrm{core}_G(U) = \mathrm{core}_G(V) = 1$ and $U \cap Z = V \cap Z = 1$.

Proof. Set $X = \mathrm{core}_G(U)$. Then

$$XV \leqslant X \cdot \bigcup_{z \in Z} U^z = \bigcup_{z \in Z} (XU)^z = \bigcup_{z \in Z} U^z = \bigcup_{z \in Z} V^z.$$

In particular $XV \cap Z \leqslant \bigcup_{z \in Z} V^z$, hence $XV \cap Z \leqslant V$ (because Z is abelian). From $G = VZ$ we get $XV = (XV \cap Z)\, V \leqslant V$, hence $X \leqslant V$. If $X \neq 1$, then it follows by Step 1 that $U = UX = V^g X = V^g$ for some $g \in G$, contradicting the assumption that G is a counter-example. Thus $X = 1$. The second assertion follows from $U \cap Z \leqslant \mathrm{core}_G(U) = 1$. Similarly for V. ∎

Step 3. There exists a subgroup W of G which contains both U and a G-conjugate of V as maximal subgroups.

Proof. Among all subgroups of G that contain U or V properly, pick one with minimal cardinality, call it W. If $W = G$, we are done. Now assume $W \neq G$. Suppose for instance that $U < W$. Then $D = \mathrm{core}_G(W)$ is nontrivial (as it contains $W \cap Z > 1$). By Step 1 we get $UD = V^g D$ for some $g \in G$. Thus $V^g \leqslant UD \leqslant W$. ∎

Let's introduce some more notation. Choose a group W according to Step 3. We may assume that U and V are both maximal subgroups of W. We already remarked that W has a nontrivial core in G. So pick a minimal (nontrivial) normal subgroup N of G which is contained in W. By Step 2 N is either contained in U nor in V. Thus, by maximality of U and V in W, we get $W = UN = VN$. Set $N_U = \mathrm{core}_W(U)$ and $N_V = \mathrm{core}_W(V)$. Note that N_U and N_V are the kernels of the action of W on the coset spaces W/U and W/V, respectively.

Since N is a minimal normal subgroup of G, it can be written as $N = S_1 S_2 \cdots S_t$, the direct product of simple groups S_i.

Step 4. Exactly one of the S_i's, say S_1, is not contained in N_U.

Proof. For $Y \leqslant W$ denote by $\bar{Y}$ the image of Y in W/N_U. Then $\bar{W}$ acts faithfully and primitively (as U is maximal in W) on the coset space W/U. Since $W = (W \cap Z)\, U$, the group $\overline{W \cap Z}$ is a cyclic transitive subgroup of $\bar{W}$. Moreover, $\bar{W}$ is not solvable by (iv), hence $\bar{W}$ is 2-transitive on W/U by theorems of Schur and Burnside [13, Theorems 25.3 and 11.7]. Because $\bar{W}$ is a 2-transitive permutation group, it has a unique minimal normal subgroup $\bar{S}$ which is either elementary abelian or simple non-abelian (see [13, Exercise 12.4]). Let S be the preimage of $\bar{S}$ in W. If a 2-transitive permutation group with cyclic transitive subgroup has an elementary abelian normal subgroup of order p^r, then $p^r = 4$ or $r = 1$, see [10, Proof of Satz 5]). Since $\bar{W}$ is not solvable, $\bar{S}$ is a simple non-abelian group. From $\bar{N} \neq 1$ (Step 2) we get that $\bar{N}$ contains the unique minimal normal

subgroup $\bar{S}$ of $\bar{W}$. Thus $\bar{S}$ is a simple normal subgroup of $\bar{N} = \bar{S}_1 \bar{S}_2 \cdots \bar{S}_t$, hence $\bar{S} = \bar{S}_i$ for some i, say $\bar{S} = \bar{S}_1$. Then $C_{\bar{W}}(\bar{S}_1) \lhd \bar{W}$. But $\bar{S}_1$ is not abelian, therefore $\bar{S} = \bar{S}_1 \not\leqslant C_{\bar{W}}(\bar{S}_1)$. This shows $C_{\bar{W}}(\bar{S}_1) = 1$, in particular $S_j \leqslant N_U$ for $j \geqslant 2$. ∎

Step 5. $W \leqslant N_G(S_1)$.

Proof. Follows from Step 4, since W permutes the S_i's and normalizes N_U. ∎

Step 6. $N_U = C_W(S_1)$.

Proof. We showed $C_{\bar{W}}(\bar{S}_1) = 1$ in the proof of Step 4, hence $C_W(S_1) \leqslant N_U$. We get the other inclusion as follows: S_1 is simple and normal in W by Step 5. Thus $S_1 \cap N_U = 1$ and therefore $N_U \leqslant C_W(S_1)$. ∎

Step 7. Exactly one of the S_i's, call it S_{i_0}, is not contained in N_V. We have $W \leqslant N_G(S_{i_0})$ and $N_V = C_W(S_{i_0})$.

Proof. We proceed as in Steps 4, 5, and 6, using that W/N_V is not solvable. This is the case because $N = S_1 S_2 \cdots S_t$ has non-trivial image in W/N_V (by Step 2), and the S_i's are simple non-abelian groups. ∎

Step 8. Every group L that contains U is self-normalizing in G.

Proof. Assume that there is an element $g \in G \backslash L$ that normalizes L. Then $L \lhd \langle L, g \rangle =: H$. Now pick a subgroup M of H that contains L as a maximal subgroup. But M/L is cyclic, contrary to (iv). ∎

Step 9. $i_0 = 1$.

Proof. First we observe that Z permutes the S_i's transitively, because G does so, W fixes S_1 (by Step 5), and $G = WZ$. Therefore $N_G(S_j) \cap Z$ is independent from j. By Steps 5 and 7 we know that W is contained in $N_G(S_1)$ and $N_G(S_{i_0})$, hence

$$N_G(S_1) = (N_G(S_1) \cap Z)\, W = (N_G(S_{i_0}) \cap Z)\, W = N_G(S_{i_0}).$$

Pick $g \in G$ with $S_{i_0} = S_1^g$. Then

$$N_G(S_1) = N_G(S_{i_0}) = N_G(S_1)^g.$$

But $g \in N_G(S_1)$ by Step 8, therefore $S_{i_0} = S_1^g = S_1$. ∎

Step 10. The final contradiction.

Proof. From Steps 6, 7, and 9, we get $N_U = N_V$. Again write $\bar{Y}$ for the homomorphic image of $Y \leqslant W$ in $W/N_U = W/N_V$. Set $\bar{C} := \overline{Z \cap W}$. From $W = (W \cap Z)\, U = (W \cap Z)\, V$ we get $\bar{W} = \bar{C}\bar{U} = \bar{C}\bar{V}$. Now use (iv) to

conclude that $\bar{U}$ and $\bar{V}$ are conjugate in $\bar{W}$. But this implies conjugacy of U and V in W, contrary to the assumption of a counter-example.

6. Examples

We believe that Theorem 4.1(1) cannot be improved considerably. The special assumption (*) on the indecomposable components of f is the translation of 5.1(iv). If we drop parts of (iv), then Lemma 5.1 admits counter-examples. In several cases corresponding polynomials can be constructed. In the examples we found these polynomials cannot be chosen with rational coefficients, so they do not contradict Theorem 4.1(1). However, they do contradict Theorem 4.1(2) and thus provide negative answers to the Question in the Introduction.

Up to now only the following construction of Fried was known; Choose a group G with $PSL_m(q) \leqslant G \leqslant P\Gamma L_m(q)$ with $m \geqslant 3$ and q a prime power, which is a monodromy group of a polynomial (there are 5 such cases, see [2]). Let Z be a Singer cycle. Let U and V be just as the stabilizer of a point and a hyperplane in the underlying projective space, respectively. Then (i), (ii), and (iii) of 5.1 are fulfilled, however U and V are not conjugate. A similar construction works with $G = PSL_2(11)$ in its representation of degree 11.

The examples just sketched fulfill the non-solvability condition on $\bar{M}$ 5.1(iv), however they fail the assumption on the complements. Even if we keep the condition on the complements, but drop the condition on the non-solvability on $\bar{M}$, counter-examples arise. The "smallest" one which yields a realization of a pair of Kronecker equivalent polynomials is as follows: Set $G = GL_2(3)$. Let Z be a Singer cycle of G, U a stabilizer of a non-zero vector, and V the image of U under transposing matrices.

To this example there corresponds a pair of polynomials that is Kronecker equivalent over $\mathbb{C}$ (and then also over a suitable number field), but not linearly related over $\mathbb{C}$. For this let a and b be two solutions of $27T^2 - 14T + 3 = 0$. Then $f(X) = (X^2-1)^3 (aX^2-1)$, $g(X) = (X^2-1)^3 (bX^2-1)$ is such a pair. One can slightly modify this example to get a counter-example to the Question from the Introduction over the field $\mathbb{Q}(\sqrt{-2})$: Replace in g the term X^2 by $-3X^2$.

7. Remarks on a Related Question

Let $f, g \in \mathbb{C}[X]$ be polynomials, and U, V, and G be the Galois groups defined as in the proof of Theorem 4.1. If f and g are Kronecker equivalent

then 5.1(iii) holds. This shows that then any $v \in V$ has a fixed point on the coset space G/U, hence V is intransitive on G/U, thus $UV \subset G$ (proper inclusion). The group theoretic property $UV \subset G$ is equivalent to $f(X) - g(Y)$ being reducible. If f and g are indecomposable and $f(X) - g(Y)$ is reducible, then the converse holds, that is f and g are even Kronecker equivalent, see [6, Lemma 3]. In the general case of decomposable polynomials however $f(X) - g(Y)$ being reducible is a much weaker condition than f and g being Kronecker conjugate. Our setup in Section 5 does not cover this more general question. There is no substitute for the induction Step 1 in the proof of Lemma 5.1. The condition $UV \subset G$ does not inherit to factor groups, in contrast to condition 5.1(iii). Fried [7, Section 2] has some results in this direction, and he also displays the difficulties arising there.

REFERENCES

1. F. DOREY AND G. WHAPLES, Prime and composite polynomials, *J. Algebra* **28** (1974), 88–101.
2. W. FEIT, On symmetric balanced incomplete block designs with doubly transitive automorphism groups, *J. Combin. Theory Ser. A* **14** (1973), 221–247.
3. W. FEIT, Some consequences of the classification of finite simple groups, *in* "The Santa Cruz Conference on Finite Groups," Proc. Sympos. Pure Math., Vol. 37, pp. 175–181, Amer. Math. Soc., Providence, RI, 1980.
4. M. FRIED AND M. JARDEN, "Field Arithmetic," Springer-Verlag, Berlin/Heidelberg, 1986.
5. M. FRIED, On a conjecture of Schur, *Michigan Math. J.* **17** (1970), 41–55.
6. M. FRIED, The field of definition of function fields and a problem in the reducibility of polynomials in two variables, *Illinois J. Math.* **17** (1973), 128–146.
7. M. FRIED, Irreducibility results for separated variables equations, *J. Pure Appl. Algebra* **48** (1987), 9–22.
8. M. FRIED, Rigidity and applications of the classification of simple groups to monodromy, II. Applications of connectivity; Davenport and Hilbert–Siegel problems, preprint.
9. M. FRIED AND R. E. MACRAE, On the invariance of chains of fields, *Illinois J. Math.* **13** (1969), 165–171.
10. B. HUPPERT, Primitive, auflösbare Gruppen, *Arch. Math.* **6** (1955), 303–310.
11. P. MÜLLER, Primitive monodromy groups of polynomials, *in* "Recent Developments in the Inverse Galois Problem," Contemporary Maths., Vol. 186, pp. 385–401, Amer. Math. Soc., Providence, RI, 1995.
12. J. F. RITT, Prime and composite polynomials, *Trans. Amer. Math. Soc.* **23** (1922), 51–66.
13. H. WIELANDT, "Finite Permutation Groups," Academic Press, New York/London, 1964.